

REMARKS

Claims:

Claims 1-66 comprise the case, independent Claims 1, 15, 29 and 40 having been amended, and Claims 51-66 newly added.

35 U.S.C. 103(a):

Claims 1-50:

Claims 1-50 stand rejected under 35 U.S.C. 103(a) based upon Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. Patent No. 4,956,769), and further in view of other patents for certain dependent claims. The additional cited patents are Davis (U.S. Patent No. 4,941,201), Wright et al. (U.S. Patent No. 6,084,969), Bapat et al. (U.S. Patent No. 6,038,563), and Hastings et al. (U.S. Patent No. 6,370,629).

A)

In the response to arguments, the Examiner stated that in the present Application, "the data the user is trying to gain access to is not kept on the authorization device. The data is stored on a device such as a magnetic tape cartridge or an optical disk on which is attached the wireless authorization device. If limitations were [sic] made in the independent claims in this manner, the claims would become patentably distinct over the cited references ***."

Accordingly, Applicant has amended each of the independent claims that had been previously submitted, Claims 1, 15, 29 and 40, to incorporate the language "separate from said data storage media" to indicate that the authorization device and the

operations performed to conduct the authorization are separate from the data storage media.

For example, Claim 1 recites "A portable security system for managing access to a portable data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, said portable security system comprising:

a wireless interface mounted in said portable data storage cartridge ***; and

a computer processor mounted in said portable data storage cartridge separate from said data storage media, and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

Applicant therefore submits that independent Claims 1, 15, 29 and 40, and all claims that depend therefrom are patentable over the cited references.

Applicant additionally submits that Applicant's claimed invention defines over the cited references for other reasons. The previous discussions of these reasons may not have been sufficiently clear, and, therefore, Applicant is not repeating those discussions, instead focussing on the following:

Anderl et al. and Smith are submitted to teach away from a fully portable security system.

In Anderl et al., the application software that provides the authorization and access operations is in an application station, and the application station and card must cooperate in order to gain access. (See page 5, lines 2-11, "The application software resides in the station and enables the retrieval and modification of information stored in the memory of the card 10. The card 10 runs an executive operating system that is accessed via a set of operating system command primitives. These command primitives manipulate a file system on the card in accordance with rules required by card security", and page 7, lines 12-19, "numbers are manipulated algorithmically to produce an authentication code which is stored in the application file on the card at the time of creation. During subsequent transactions, this code must be favorably compared to a similar code generated independently by the station." (emphasis added)).

Only at a special station is a "MASTER ISSUER", "SUPER USER or DEVELOPER" allowed to employ passwords to access various login levels that are checked internally. From the above, it appears that this special station also cooperates with the card to gain access to the card and provide the command primitives. "The fourth level of security is that retained by the MASTER ISSUER. It is at this level that the card is formatted and from which it is issued. *** Each account in this example is handled by a separate file on the card and only persons or programs with the proper credentials for a particular file may access that file at

an appropriate application station." (page 8, lines 6-15)
(emphasis added).

Smith is "a value based security system in a computer host system." (column 4, lines 25-27) (emphasis added).

Applicant's claims are submitted to claim a complete security system that is in the data storage cartridge and is portable with the cartridge, not dependent on an application in a station to provide the authentication, and not requiring a special station for various user activities. For example, Claim 1 recites "A portable security system for managing access to a portable data storage cartridge, ***, said portable security system comprising:

a wireless interface mounted in said portable data storage cartridge ***; and

a computer processor mounted in said portable data storage cartridge separate from said data storage media, and coupled to said wireless interface; *** said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

Applicant's dependent claims emphasize this difference, detailing the various activities that a user may conduct, if authorized, and detailing the authorization process.

Accordingly, Applicant believes the present invention distinguishes over the cited patents and respectfully requests that the Examiner allow Applicant's Claims 1-50 under 35 U.S.C. 103.

B)

Applicant's new Claims 51-66 also emphasize that the portable security system resides in the cartridge, and is therefore truly portable.

For example, independent Claim 51 recites "A portable data storage cartridge, comprising:

a wireless interface mounted in said portable data storage cartridge configured to receive power and data from, and send data to, a data storage drive, when in said data storage drive; data storage media; and

a portable security system that resides in said portable data storage cartridge, comprising:

a computer processor system residing in said portable data storage cartridge and configured to communicate with said wireless interface, and configured to receive power from said wireless interface; and

a security system configured for operation of said portable data storage cartridge computer processor system arranged to authenticate each of separate users by combining a user authentication message received via said wireless interface, with a user identifier of a plurality of user identifiers previously stored by said computer processor system, said user identifiers comprising at least a unique

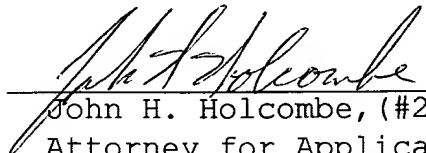
Appl. No.: 09/435,899
Amdt. dated: December 1, 2005
Reply to Office action of 09/12/2005

user identifier for each authorized user, said combining in accordance with a predetermined algorithm of said security system." (emphasis added).

Applicant respectfully submits that the above argument relating to the need for the Anderl et al. station to gain access to the card and to provide the command primitives, and relating to the Smith host based system indicates that Anderl et al. and Smith teach away from Applicant's Claims 51-66.

Accordingly, Applicant believes the present invention distinguishes over the cited patents and respectfully requests that the Examiner allow Applicant's Claims 51-66 under 35 U.S.C. 103.

Respectfully submitted,
P. J. Seger

By: 
John H. Holcombe, (#20,620)
Attorney for Applicants
From: IBM Corporation
Intellectual Property Law
8987 E. Tanque Verde Rd. #309-374
Tucson, AZ 85749
Telephone: (520) 760-6629

JHH/cw